RD&E

CENTER

Technical Report

No. 13548

SYSTEM HAZARD ANALYSIS OF TACOM'S CREW STATION/ TURRET MOTION BASE SIMULATOR

JANUARY 1992

By Alexander A. Reid
U.S. Army Tank-Automotive Command
ATTN: AMSTA-RYA
Warren, MI 48397-5000

U.S. ARMY TANK-AUTOMOTIVE COMMAND
RESEARCH, DEVELOPMENT & ENGINEERING CENTER
Warren, Michigan 48397-5000

NOTICES

This report is not to be construed as an official Department of the Army position.

Mention of any trade names or manufacturers in this report shall not be construed as an official endorsement or approval of such products or companies by the U.S. Government.

Destroy this report when it is no longer needed. Do not return it to the originator,

REPORT DOCUMENTATION PAGE

1. REPORT NO.

2.

3. Recipient's Accession No.

4. Title and Subtitle
SYSTEM HAZARD ANALYSIS OF TACOM'S CREW STATION/TURRET MOTION BASE SIMULATOR (CS/TMBS)

5. Report Date
Jan 1992

6.

7. Author(s)
Alexander A. Reid

8. Performing Organization Rept. No.

9. Performing Organization Name and Address
U.S. Army Tank-Automotive Command
ATTN: AMSTA-RYA
Warren, MI 48397-5000

10. Project/Task/Work Unit No.

11. Contract(C) or Grant(G) No.
(C)
(G)

12. Sponsoring Organization Name and Address

13. Type of Report & Period Covered
FINAL

14.

15. Supplementary Notes

16. Abstract (Limit: 200 words)

This is a System Hazard Analysis of TACOM's Crew Station/Turret Motion Base Simulator. This report presents a general overview of system hazards as well as a detailed breakdown of all hazards, their severity and probability of occurring, and an explanation of the safety backups.

17. Document Analysis a. Descriptors

b. Identifiers/Open-Ended Terms

c. COSATI Field/Group

18. Availability Statement

19. Security Class (This Report)
Unclassified

20. Security Class (This Page)
Unclassified

21. No. of Pages
39

22. Price

(See ANSI-Z39.18) See Instructions on Reverse

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF TABLES

1.0 INTRODUCTION

This report provides a System Hazard Analysis (SHA) of the Crew Station/Turret Motion Base Simulator (CS/TMBS) located at the United States Army Tank-Automotive Command (TACOM) in Warren, Michigan. It also provides the U.S. Army Test and Evaluation Command with component descriptions and hazard analyses of the CS/TMBS.

The Crew Station/Turret Motion Base Simulator was designed to include provisions for safeguarding personnel and equipment. Safety devices have been located on the equipment where necessary and are described in the Contraves USA Manual No. IM-27751, "INSTRUCTION MANUAL FOR TACOM."

This System Hazard Analysis (SHA) is submitted concurrently with a Safety Analysis Report (SAR) in an effort to obtain a safety release for the Crew Station/Turret Motion Base Simulator.

The scope of this System Hazard Analysis is the systematic assessment of real and potential hazards associated with the subsystems of the Crew Station/Turret Motion Base Simulator. This SHA was conducted on the available system concept data in an attempt to identify hazards and to then direct design efforts toward the elimination or control of the identified hazards.

2.0 OBJECTIVES

The primary goal is to obtain a safety release from the U.S. Army Test and Evaluation Command for the Crew Station/Turret Motion Base Simulator itself. Different payloads (crewstations) must be individually safety certified. This report is issued in conjunction with TACOM Technical Report No. 13549, "SAFETY ASSESSMENT OF TACOM's CREW STATION/TURRET MOTION BASE SIMULATOR" and Contraves USA Manual No. IM-27751, "INSTRUCTION MANUAL FOR TACOM" in an attempt to satisfy MIL-STD-882B.

3.0 CONCLUSIONS

All known safety hazards have been evaluated throughout the design and development of the Crew Station/Turret Motion Base Simulator. The system is considered safe to operate providing the procedures stated in the "INSTRUCTION MANUAL FOR TACOM" are followed.

The safety devices and procedures for the Crew Station/Turret Motion Base Simulator will reduce the probability of injury to occupant or damage to equipment to the levels dictated in MIL-STD-882B.

There will be communications between the crewstation and the CS/TMBS operator at all times during a test. The crewstation will also have an emergency stop button in ready access to provide the crew a means of stopping the test. It will be assumed that the crew will meet all requirements imposed by the safety certification of the crewstation.

4.0 RECOMMENDATIONS

Upon issuance of a safety release for the Crew Station/Turret Motion Base Simulator, it is suggested that the Safety Office at TACOM be given power to approve various test setups and issue safety releases for them.

5.0 DISCUSSION

5.1 System Description

The CS/TMBS is a high-performance, six-axis motion simulator capable of handling payloads of up to 25 tons. It recreates the dynamic motions a vehicle would experience traveling over cross-country terrain, while being capable of handling a wide range of crew stations from M1 turrets to smaller crew stations equipped with computer-generated imagery systems.

The simulator is intended to replace costly field testing of vehicles in development (or being modified) with a controlled laboratory environment in which to conduct testing.

The CS/TMBS is considered a "Stewart Platform," named after the researcher who developed the concept in the late sixties. The basis of the Stewart Platform was developed for flight simulators and has been used for many applications in laboratory simulation. One feature which makes the CS/TMBS unique among the other known Stewart Platform systems is the capability to handle heavy loads with a bandwidth motion of 5 Hz.

The CS/TMBS was designed and built by Contraves USA and assembled jointly by Contraves USA and TACOM. All control compensation was performed by TACOM. The CS/TMBS is expected to open doors to new research, development and testing in the areas of gun/turret drive tracking and stabilization systems along with man-in-the-loop testing. One potential feature of the CS/TMBS is the ability to test and study the soldier-machine interface while in a dynamic environment.

5.2 Major Subsystems and Components

The CS/TMBS is described under the following equipment categories:

- Frame Structure
- Supervisor Computer
- Safety Monitor Computer
- Interlock Chassis
- Motion System
- Inertial Measurement Unit

- Analog I/O
- AD-100 Computer Interface
- Array Processor
- Encoder Servo Processors
- Hydraulic System

5.3 Analysis Summary

The analysis results presented in the following pages address the hazard potential to the Crew Station/Turret Motion Base Simulator should there be a failure in any of the subsystems.

5.4 Assignment of Risk Assessment Codes

The accompanying analysis sheets contain hazard severity levels, hazard probability levels and Risk Assessment Codes (RAC). The hazard probability levels and RAC are from AR 385-10 Interim Change No. I01. The hazard severity levels are from MIL-STD-882B, so that system damage and personnel injury can be included in the definition and reflected in the hazard assessment.

HAZARD SEVERITY

a. Category I - Catastrophic. Death or permanent total disability; system loss, major property damage.

b. Category II - Critical. Permanent partial disability or temporary total disability in excess of three months; major system damage, significant property damage.

c. Category III - Marginal. Minor injury, lost workday accident, or compensable injury or illness; minor system damage, minor property damage.

d. Category IV - Negligible. First aid or minor supportive medical treatment; minor system impairment.

HAZARD PROBABILITY

a. Frequent. Likely to occur frequently in life of system, item, facility, etc.

b. Probable. Will occur several times in life of item.

c. Occasional. Likely to occur sometime in life of item.

d. Remote. Unlikely, but can reasonably be expected to occur.

e. Improbable. Unlikely to occur, but possible.

RISK ASSESSMENT CODES

1 - Critical

2 - Serious

3 - Moderate

4 - Minor

5 - Negligible

5.5 Safety and Interlock System

The CS/TMBS system has multiple levels of safety interlocks to assure the safety of both personnel and equipment. The interlock system is divided into five subsystems with overlapping functions to achieve a high level of hazard protection. Figure 1 shows an overall view of the safety and interlock system.

The safety interlocks are distributed between:

- Interlock Chassis
- IMU Chassis
- ESP Cards
- Safety Monitor Equipment

The CS/TMBS control system supports two types of aborts when a fault is detected.

1. Hard Abort - Hard aborts are implemented through the Interlock Chassis and cause an immediate shutdown of the simulator by aborting the hydraulic control circuits. Hard aborts are used for fault conditions that could be an extreme or immediate hazard. Conditions that could cause the system to be uncontrollable also warrant a hard abort. The following action occurs when a hard abort is initiated:

- Actuator abort valves open, limiting actuator pressures.
- Servo shutoff valves close, isolating the actuators from the servo valves.
- System supply valves close, isolating the CS/TMBS system from the hydraulic power supply.

2. Soft Abort - A soft abort is a computer controlled shut-down in

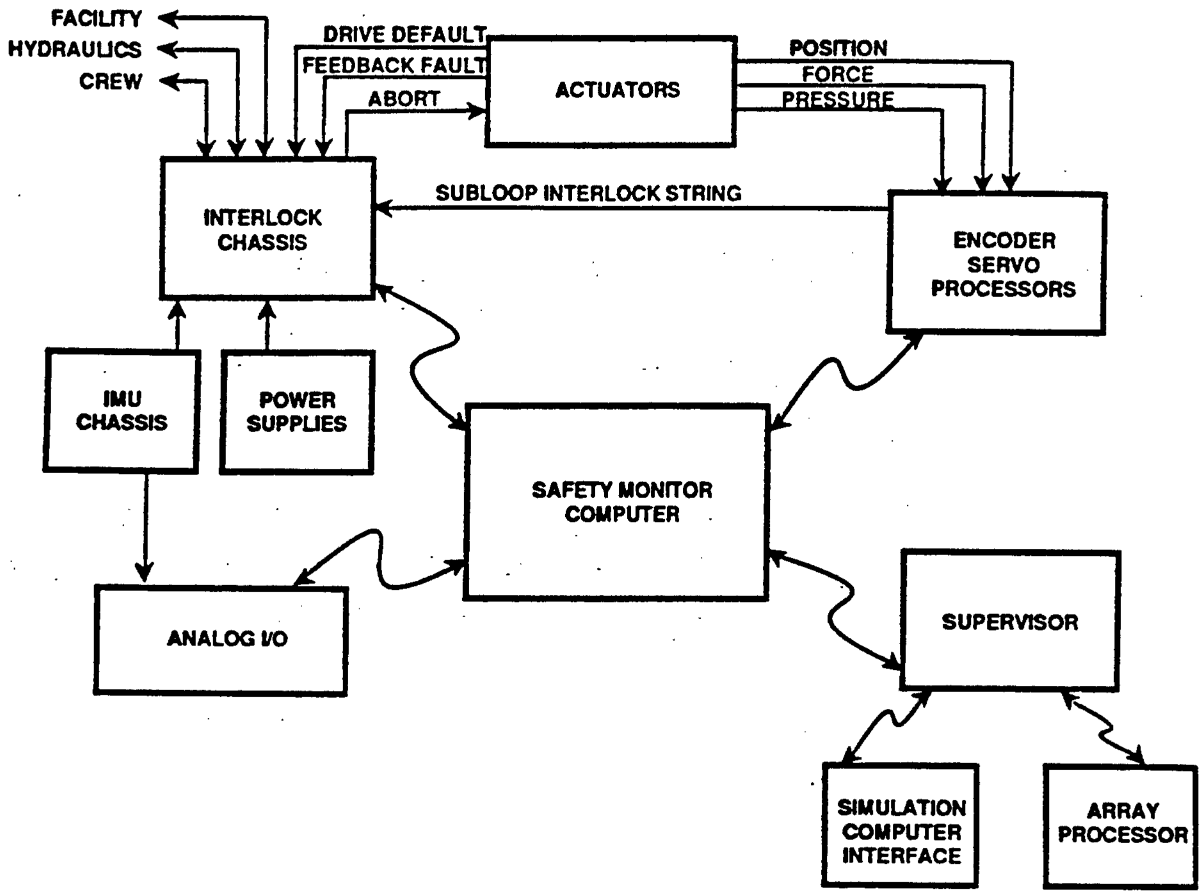

Figure 1. Safety and Interlock System Block Diagram

response to a nonimminent hazard or recoverable error. When a soft abort error condition occurs, the CS/TMBS controls cause the system to:

- Return the platform to a neutral position and orientation.

- Lower the platform to the settled position and abort hydraulics.

5.5.1 Interlock chassis. The Interlock Chassis directly controls the CS/TMBS system hydraulics to ensure a safe and rapid shutdown in the event of a system fault. Various function cards in the Interlock Chassis form the hardware interlock string, a relay ladder that controls the hydraulic solenoid valves via the Interlock Control box. The hydraulics cannot be energized until the hardware interlock string is closed (satisfied). A hard abort occurs when the interlock string opens due to a fault detected by one of the interlock function cards.

The Interlock Chassis contains three types of printed circuit cards, such as:

- Interlock Card (4)
- Analog Limit Card (6)
- Control and Status Card (3)

Not all of these cards are in the hardware interlock string, however, they all serve a function in the safe control of the CS/TMBS.

5.5.1.1 Interlock Card Functions. The Interlock Cards connect to various contact closures and TTL signals in the CS/TMBS system. The following functions are in the hardware interlock string:

- Retract Limit Switches (6)
- Extend Limit Switches (6)
- Solid State Relay (SSR) Fault
- IMU Linear Acceleration Limit
- IMU Angular Acceleration Limit
- IMU Angular Rate Limit
- Inertial Switch
- 115 VAC Power Fail
- 24 VAC Power Fail
- ESP Interlock String
- Console Emergency Stop
- Facility Emergency Stop
- Crew Emergency Stop
- Facility Pressure Switch
- Return Pressure High
- Return Valve Closed
- Service Jack Interlock
- Connector Interlock
- System Pressure Critical

Interlock hardware overrides the Retract Limit switches until the system is out of the retract limits. Likewise, the System Pressure Critical (<1500 psi) interlock is bypassed until after the hydraulic pressure is stabilized. The SSR fault shows a failure in one of the

Solid State Relays that drive the hydraulic solenoid valves. The IMU limits indicate excessive acceleration or rate has been detected in the IMU Chassis. Provision is made for a multi-axis inertial switch to be mounted in the crew compartment as a back-up inertial interlock. The switch is calibrated to trip at a preset G level along its X, Y, and Z axis. The 115 volt AC Power Fail aborts the hydraulics and control system before the DC power supply voltages drop to a critical level. A 24 volt AC power failure inherently aborts all solenoid valves, but its inclusion in the interlock string assures that the ESP's and Safety Monitor Computer detects the failure. The ESP Interlock String input is from a series connection of the ESP interlock relays. This direct path to the Interlock Chassis provides redundancy in case of a multi-bus communication failure. Section 5.5.2 details the ESP interlocks. The Emergency Stop buttons allow the system operator at the console, facility personnel near the simulator or the tank crew to affect an immediate CS/TMBS system abort. Prior to starting the system, facility pressure must be sensed on the HPS side of the CS/TMBS supply valves. The absence of facility pressure while the system is active will cause an abort. The CS/TMBS system is supplied with a shutoff valve at the return manifold to facilitate hydraulic maintenance operations. The Return Valve Closed switch and Return Pressure High switch guarantee that the system cannot be operated without full return flow capacity. Provisions are made for the placement of service jacks in lieu of the hydraulic actuators to support the platform while maintenance and repair procedures are performed. The Service Jack Interlock prevents system operation while the service jacks are in.

Certain Interlock Card inputs are not connected to the hardware interlock string, but provide status to the Safety Monitor Computer (SMC) to:

1. Determine the current operational mode.

2. Provide status information to the operator.

3. Initiate soft aborts through the Safety Monitor Computer.

These Interlock Card status inputs are:

- Cylinder Enable (6)
- Pressure High
- Pressure Low
- Temp High
- Temp Low
- Oil Low
- Filter Clogged
- Deadman Switch
- Gate Open
- Crane Proximity
- Remote Enable

The Safety Monitor Computer (SMC) initiates a soft abort when the Pressure High, Pressure Low, Oil Temperature High, Oil Reservoir Low, Filter Clogged, Deadman Switch, Gate Open, Crane Proximity, Access

Platform Retracted or Remote Enable interlocks are not satisfied. Temperature Low is for operator information only. It aids in the diagnosis of problems that might be related to the oil being below normal operating temperature.

The Motion Consent switch in the crew compartment must be pressed simultaneously with the Hydraulic Start switch at the control console in order to open the supply valve and commence system operation. When the system is to be used without a crew, the Crew Disable keyswitch at the Interlock Control Box bypasses the Motion Enable switch. The Remote Enable switch is an optional contact closure provided by customer equipment to enable system start-up and initiate soft aborts.

5.5.1.2 Analog Limit Card Functions. The Analog Limit cards control the safety interlock system based on absolute high and low limits or a tracking comparison between two signals. These interlock functions respond based on preset high and low voltage limits:

- +5 volt supply
- +15 volt supply
- -15 volt supply
- +15 volt backup supply
- -15 volt backup supply
- +28 volt supply
- +12.8 volt Moog Rack 1 supply
- -12.8 volt Moog Rack 1 supply
- +12.8 volt Moog Rack 2 supply
- -12.8 volt Moog Rack 2 supply
- +12.8 volt Moog Rack 3 supply
- -12.8 volt Moog Rack 3 supply
- Actuator Force Limit

<u>Note</u>: Moog Controls Inc. is the actuator supplier.

All of the above limits are safety critical and therefore in the hardware interlock string except the ±15 volt backup supplies and the +28 volt supply for the IMU angular rate sensor. These two interlocks cause soft aborts through the Safety Monitor Computer. The Actuator Force limits may be thought of as absolute positive and negative (extend and retract) force limits.

The following analog limits are designed as tracking window comparisons of two signals. They are used to detect actuator transducer failures and are included in the hardware interlock string.

- Actuator Drive Fault (18)
- Actuator Feedback Fault (6)

An Actuator Drive Fault occurs if the servo valve spool position does not correspond with the valve drive signal. Spool position is measured by an LVDT on the last stage of the servo valve. The valve drive signal for each group of three servo valves is subtracted from the three demodulated spool position signals. The resultant signal is low pass filtered to compensate for the valve bandwidth and the high and low limits are set to allow an error window. The Drive Faults are bypassed until pressure is applied to the valves so that the hydraulics can be started. With pressure applied, the valve drives and feedback should track regardless of whether the valve is enabled (servo shutoff valves open). All servo valves are exercised to detect failures prior to opening the servo shutoff valves.

An Actuator Feedback fault occurs if the force measurement from the actuator strain gauges does not compare with the actuator differential pressure (i.e., force measurement). The difference signal is filtered to compensate for transducer bandwidth and high and low tracking limits are set. The redundant force and pressure transducers detect transducer failure as well as excess friction in the actuator. Actuator friction causes the differential pressure to exceed the force applied to the platform. The Actuator Feedback faults are bypassed until after platform liftoff because the comparison is not valid until this time.

5.5.1.3 Control and Status Card Functions. The Control and Status cards have power drivers to control lamps, relays, and solenoids. They also have status inputs that can be read by the Safety Monitor Computer, but are not part of the hardware interlock string.

All of the Operator Panel indicators are computer controlled via the Control and Status Card. These lamps are:

- Low, Med, High Dynamics
- Interlock GO
- HPS ON
- Hydraulic Start (2)
- Hydraulic Stop (2)
- Cylinder Mode Indicators (6)
- Axis Mode Indicators (6)

Each lamp is also connected to a corresponding status input that detects filament continuity when the lamp is turned off. This feature is used for the computer controlled lamp test. The Safety Monitor Computer also tests to verify that the lamp drivers are functional.

The following relays used in the safety interlock system are controlled by Control and Status card power drivers:

- Solenoid Power Enable
- HPS Start
- Supply valve
- Audible Warning
- Retract Access Platform
- Servo A Enable
- Servo B Enable
- Servo C Enable
- Test Abort A
- Test Abort B
- Inertial Switch Test

Solenoid Power Enable energizes a solid state relay (SSR) that enables the 24 VAC solenoid valve power transformer. The Safety Monitor Computer (SMC) enables the 24 VAC prior to hydraulic startup. When this is enabled, three red warning strobe lights on the platform begin flashing to warn that hydraulic turn-on is imminent. When the system is ready to start, the SMC issues the Retract Access Platform command. This is used to signal personnel to retract the entry structure. The SMC sounds an Audible Warning horn (on the Interlock Control Box) prior to enabling the hydraulics. The SMC then issues the HPS start and when all hardware and software interlocks are satisfied, it opens the CS/TMBS system supply valves. The Inertial Switch Test is a self-test to verify that the inertial switch safety interlock device is installed in the crew compartment.

The Servo A, B, and C Enable commands open the corresponding servo shutoff valves at the output side of the servo valves. The quantity and selection of active servo valves is controlled by the SMC through relays on the Control and Status Card, which are wired into the hardware interlock string. For safety reasons, (redundancy) each actuator has two independent sets of abort valves. The Test Abort A and Test Abort B outputs allow the SMC to test each group independently.

Three of the Control and Status Card drivers are wired to the IMU chassis:

- IMU Self Test
- IMU Linear Test
- IMU Limit Reset

IMU Self-Test is activated to perform either the linear or angular self tests. When the IMU Linear Test output is active, the IMU electronics simulate simultaneous X, Y, and Z acceleration. The angular self test is performed when the IMU Linear Self Test output is inactive. This test mode simulates simultaneous yaw, pitch and roll acceleration.

The SMC monitors the following Operator Panel switches through status inputs on the Control and Status Card:

- Remote/Local Keyswitch
- Motion Enable
- Hydraulic Stop
- System On/Off Keyswitch
- Hydraulic Start
- Power On/Off Switch

The system response to these switches is entirely under software control. The Power On switch is interlocked with the CS/TMBS system pressure switch to prevent the system from being turned off while the hydraulics are on. Without pressure, the Power OFF will turn the Power Supply Chassis off. If the hydraulics are on, Power OFF will cause a soft abort and the Power Supply will remain on until system pressure has dropped.

5.5.2 ESP Interlocks. Each of the six Encoder Servo Processor (ESP) cards has a relay contact which is part of the safety interlock string. The ESPs will close their portion of the interlock string only if unsafe conditions have not been detected. When an ESP detects an unsafe condition, the relay will open, breaking the interlock string. Only after the platform has settled to the level degrees position will the ESP then allow the supervisory processor to reset the error which opened the interlocks. After the error has reset, the ESP will once again close its portion of the interlock string.

The following software interlocks are implemented in the Encoder Servo Processor:

- Position Feedback Limit
- Force Feedback Limit
- Power Supply Limits
- Watchdog Timer
- Rate Estimate Limit
- Actuator Friction Limit
- DAC to ADC Feedback

The position feedback, rate estimate, and force feedback are software limits. The position feedback limit is a backup to the actuator limit switches. In operation, the position feedback, actuator rate estimate, and force feedback are compared against upper and lower limits. If any programmed limit is exceeded, an abort routine is initiated to open the ESP interlock relay.

The actuator friction is computed as the difference between the force feedback and the pressure feedback. If the actuator friction becomes unacceptably large, or a sensor failure occurs, an abort will be initiated.

The power supply voltages presented to the ESPs are periodically read by the onboard analog to digital converter and compared against upper and lower limits. If a supply voltage is found to be out of tolerance, the ESP will initiate an abort.

Additionally, the output of the digital to analog converter is periodically read by the analog to digital converter. If the difference exceeds a programmed limit, the ESP will abort the system.

The software watchdog is a re-triggerable one-shot that must be periodically triggered by the ESP software. If the ESP software malfunctions, the watchdog will time out and open the interlock string, aborting the system.

5.5.3 IMU Chassis. The IMU Chassis hardware is designed to open the safety interlock string if any of the following faults occur:

- Linear Acceleration Limit
- Angular Rate Limit
- Angular Acceleration Limit

The linear and angular acceleration limits are derived from the IMU outputs as described in Section 5.1.1.4 of the TACOM Instruction Manual. The IMU outputs are processed by circuits in the IMU Chassis to produce voltages proportional to the linear and angular acceleration vectors. If these voltages exceed a preset limit proportional to a value greater than 4g or 30 rad/sec^2, the interlock string is opened. The IMU accelerometers are mounted equidistant from the turret axis so that the IMU electronics can measure accelerations at the turret center. The Safety Monitor Computer performs self-tests and continuous operational monitoring of the IMU outputs.

The IMU Chassis also processes the signals from the IMU angular rate sensor and aborts the system if excess angular rate is detected.

5.5.4 Safety Monitor Computer. The Safety Monitor Computer (SMC) is a single board computer that resides in the Control Chassis Multibus card cage. The function of the safety monitor is to gather operational status and data from the control system commands and feedback to determine if the system is operating properly. Among other things, the safety monitor checks the CS/TMBS positions, rates, and accelerations to determine that the platform is operating within the design and man-rating limits. Figure 2 shows a simplified block diagram of the SMC software.

Before the hydraulics can be enabled, the SMC activates the self-test function on the IMU accelerometers to assure that they are operating properly. After the self-test, the SMC takes readings of the IMU and compares them against a set of software limits to ensure that the accelerations are not exceeded. If these limits are exceeded, then a soft abort is initiated.

The SMC also monitors the status of all inputs to the Interlock Chassis. The SMC will force an abort if any of the Interlock Chassis inputs that are in the interlock string show incorrect status. In this capacity, the SMC provides redundancy to other hardwired system interlocks. After each interlock test loop, the SMC is required to retrigger one-shots in the interlock chassis to keep the interlock string closed. This feature prevents software failures from compromising the system safety.

The SMC also monitors itself, the supervisor computer and the ESPs to ensure that the system is operating properly. The following faults will cause the SMC to force a hard abort:

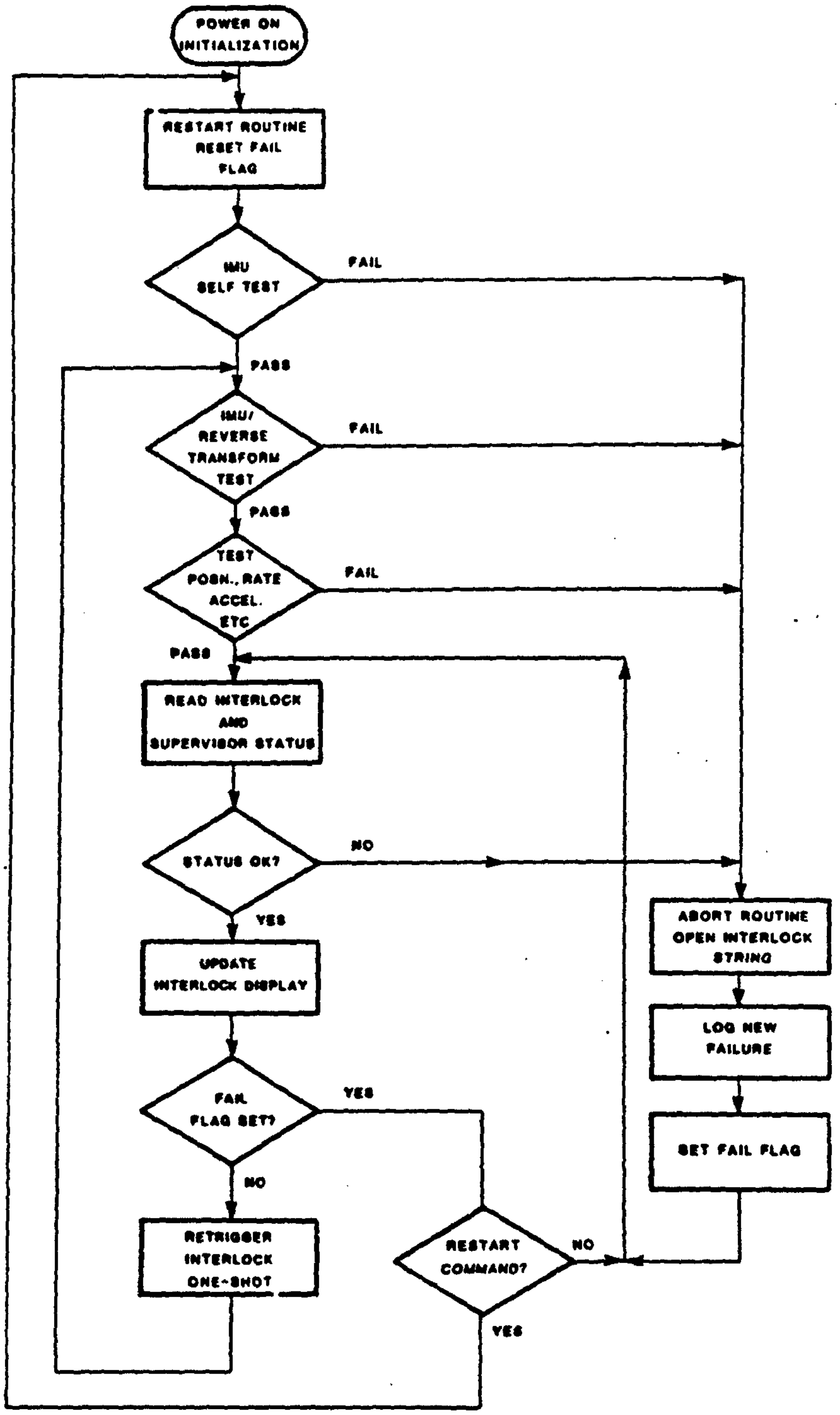
POWER ON INITIALIZATION
RESTART ROUTINE RESET FAIL FLAG
IMU SELF TEST
FAIL
PASS
IMU/ REVERSE TRANSFORM TEST
FAIL
PASS
TEST POSN., RATE ACCEL. ETC
FAIL
PASS
READ INTERLOCK AND SUPERVISOR STATUS
STATUS OK?
NO
YES
UPDATE INTERLOCK DISPLAY
FAIL FLAG SET?
YES
NO
RETRIGGER INTERLOCK ONE-SHOT
RESTART COMMAND?
NO
YES
ABORT ROUTINE OPEN INTERLOCK STRING
LOG NEW FAILURE
SET FAIL FLAG

Figure 2. Safety Monitor Software Block Diagram

- Multibus watchdog (Multibus access timeout)
- Interprocessor communication watchdog
  - Supervisor/Analog I/O checks
  - SMC check of Supervisor Runtime Counter
  - Supervisor check of SMC Runtime Counter
  - ESP communication error
- Memory Parity Error
  - Supervisor memory failure
  - SMC memory failure
- Memory Lost Error
  - Supervisor code memory failure
  - SMC code memory failure

The SMC will abort the system based on the following ESP error conditions:

- Position change when platform should be motionless
- Rate trip
- Force feedback limit
- ESP software watchdog (1 ms)
- Multi-bus watchdog
- A/D data not within acceptable limits
- Friction trip
- Upper position limit
- Lower position limit
- Special lower position limit (when applicable)
- CPU traps (any illegal instruction)

The SMC will initiate a soft abort if any of the following conditions are detected:

- ESP Command Limit
- Software Rate Limit
- Software Acceleration Limit
- Turret Weight Test Failure
- ID code mismatch during remote scenario
- Array Processor DMA complete timeout
- System command timeout on AD100 link
- 10 ms System-Tick Timeout
- Illegal Mode Change
- Crane Proximity
- Power ON/OFF Switch OFF
- System ON/OFF keyswitch OFF
- Remote Enable Off
- Hydraulic Temperature High
- 15 Volt Backup Supply Failure
- 28 Volt Supply Failure
- Filter Clogged
- Deadman Switch Open
- Gate Open
- Hydraulic Pressure High
- Hydraulic Pressure Low (not critical)

A secondary function of the Safety Monitor Computer is to log failures as they occur. They may be displayed after a failure to aid in tracing the cause of a fault. The SMC also displays the status of all the hardware and software interlocks on the operator console CRT. Table 1 lists some of the system status information that is available at the operator console. All "system go" status indicators are green and "no-go" status indicators are displayed in red so the operator can tell at a glance if the system is operational. The first interlock function to cause the hydraulics to shutdown during system operation will be displayed on the CRT screen to aid in fault diagnosis.

The SMC also is used as the operator communication link to the system by controlling the CRT display and accepting operator commands from the keyboard.

5.6 System hazard analysis. The following pages outline specific failures, hazard probabilities and severity and provide a flow-chart showing related backup systems.

Table 1. Status Display Summary

System Status

System (OFF)(ON)
(Low)(Med)(High) Dynamics
(Local)(Remote) Mode
EXT System Ready
X Position
Y Position
Z Position
Roll Angle
Pitch Angle
Yaw Angle

Hydraulic Status

Pressure (OFF)(ON)
Valve (Closed)(Open)
Pressure (Low)(High)
Filter Differential Pressure
Oil Temperature High
Oil Level Low

Interlock Status

Emergency Stop
Motion Consent (OFF)
Dead Man Switch Disable
Remote Stop
Gate Open
Step Stow Lock
Power Supply Limit
Crane Proximity
Acceleration Limit

Actuator Status

Subloop Trip
Position Limit
Rate Limit
Acceleration Limit
Pressure Limit
Valve Drive Fault
Feedback Sensor Fault

SYSTEM CS/TMBS

SUBSYSTEM FRAME STRUCTURE

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Structural Failure of Platform or Swivel Joints	Startup and operation	Fatigue or excessive stress and strain	Ranges from minor cracks to complete failure of structure	I	E	5	The platform is designed to handle 50,000 lbs @5g with a factor of safety of 2.0. Other design criteria include factor of safety of 4.0 with worst case loads of 4g vertical and 3g arbitrary direction with simultaneous 10 rad/sec^2 accelerations. The swivel joint assemblies were stressed to four times the maximum strut load of 115,000 lbs. The remainder of the platform is stressed using 16 g's vertical, 12 g's lateral along x, and 12 g's lateral along y corresponding to the required 4g vertical and 3g arbitrarily directed accelerations. In addition, the platform endurance limit with a 50,000 lb turret installed is ±2.25 g's in all directions at the 99.9% confidence level. Refer to the Contraves USA manual "TACOM PLATFORM FINITE ELEMENT ANALYSIS RESULTS", prepared under Contract DAAED7-87-C-R011.
Failure of Hydraulic Actuators	Startup, operation and shutdown	Fatigue or excessive stress and strain	Ranges from cracks in the actuator rod to complete failure including buckling of the rod	II	E	5	The actuators are specifically designed by Moog Corporation to the load tolerances set forth for this simulator. They meet all industry quality standards.

SYSTEM CS/TMBS

SUBSYSTEM SAFETY MONITOR COMPUTER

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of Safety Monitor Computer	Startup, Operation and Shutdown	Computer Hardware Failure	Loss of soft abort capability, loss of redundancy in safety interlock string	IV	D	5	With a failure of the safety monitor computer, all safety shutdowns monitored by the SMC will still cause a shutdown, but a hard abort will occur instead of a soft abort. Failure of a computer will most likely occur upon power up, and in this case the CS/TMBS will be unable to turn on, thus removing the most likely instance of SMC failure. If failure does occur during operation, the one-shot timers which the SMC re-triggers every 10 ms will not be reset, thus causing a hard abort.

SYSTEM CS/TMBS

SUBSYSTEM SUPERVISOR COMPUTER

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of Supervisor Computer	Startup, Operation and Shutdown	Computer Hardware Failure	Loss of the Supervisor Computer	IV	D	5	The Supervisor Computer performs four main functions: (1) Command generator - determines the appropriate acceleration that should be applied during the next time interval. Normally, the command will equal the demand signal. When the rate and acceleration limits are lowered, the command will be lower than the demand signal. (2) Forward Kinematic Model - performs the direct kinematic transformation from platform positions and attitudes to link demands. (3) Forward Dynamic Model - The body rates, accelerations, torques and forces are computed resulting in an estimation of the link forces. (4) Inverse Kinematic Model - accepts the link lengths and rates and solves the non-linear system of equations to produce platform position/attitude and rates. Should this computer fail for any reason, the Safety Monitor Computer along with various hardware interlocks would detect travel errors (most likely increased acceleration, also tracking error) and perform an orderly and safe shutdown. *Once again, a computer is most likely to fail upon power-up*, which would not allow the CS/TMBS to become operational, thus removing the most likely instance of failure.

SYSTEM CS/TMBS

SUBSYSTEM INTERLOCK CHASSIS

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of Hardware Interlock String Items	Startup, Operation and Shutdown	Failure of relay, loss of power, misc. electrical problems	Loss of ability to detect safety failures, emergency stop actions and more (all items described in Section 5.5.1)	IV	D	5	The loss of an item in the hardware interlock string will not in itself cause any damage or have a noticeable effect on the functioning of the CS/TMBS. The failure of the interlock relays will itself cause a break in the interlock string which will be detected by the Safety Monitor Computer, thus causing a shut-down of the system. Because of redundancy in the monitoring of possible hazards, a failure which is not detected by the interlock chassis would be noticed by either the Safety Monitor Computer or the Encoder Servo Processor Cards. Loss of power itself would automatically cause a hard abort due to the supply valve closing, the abort valve opening (4 per cylinder), and the servo shutoff valves closing, thus causing the actuators to slowly retract all the way down.
Failure of power supplies, ±15v, +5v, 120v, etc.	Startup, operation and shutdown	Power supply burnout	Loss of servos, electronics, computers	III	D	5	Same as above, i.e. hard abort, abort valves open, servo shutoff valves close, supply valves close, simulator slowly retracts. Big capacitors provide early servo control for ≈100 mSec.

SYSTEM CS/TMBS

SUBSYSTEM MOTION SYSTEM

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Loss of integrity of input terrain signal	Operation	Error in the data file, operator select incorrect data, problem with transmission of data, etc.	Unsuspected movement of the simulator, possibly high accelerations	III	C	4	To avoid transmitting the wrong data file from the AD-100 computer to the CS/TMBS, the operator is required to enter an identification number when selecting the file to transmit. If it does not match the identification number of the file on the AD-100, no transfer will take place. All data is then digitally filtered (to software selectable limits) and then limited in value for position, rate and acceleration (again to software selectable limits). Thus, there is a triple safeguard on the validity of the data itself. If there was unwanted movement, the IMU unit would detect overlimit positions, rate or accelerations and shutdown the CS/TMBS. The crew in the payload, the observer by the simulator, along with the operator would also be able to stop the simulator by pressing the emergency stop button.
Loss of feedback signals	Startup, operation and shutdown	Break in the data path due to instrument failure or loss of transmission	Running as an open loop system, eventual loss of control of simulator	IV	D	5	The loss of feedback would immediately be detected by the interlock chassis and also the ESP cards, which would force an immediate shutdown before loss of control occurs. Even if the simulator began to run away, the Inertial Measurement Unit (IMU) would detect over-limit conditions and shut down the CS/TMBS. The crew in the payload, the observer by the simulator, along with the operator would also be able to stop the simulator by pressing the emergency stop button.
Abrupt movement or spike in travel	Startup, operation and shutdown	Bad data along with failure of filters	Sharp movement of the simulator	III	D	5	For this to happen there would first have to be bad data sent into the simulator. The filters which smooth the data would have to fail, then the software limits for position, rate and acceleration would also fail. If all this did happen, the IMU would detect the acceleration and shutdown the simulator immediately. Extremely unlikely. The crew in the payload, the observer by the simulator, along with the operator would also be able to stop the simulator by pressing the emergency stop button.
Position, rate or acc overtravel	Operation	Bad data, operator error	Reaching the extend or retract limits of the actuators, abrupt stop will occur, possible damage to system	III	D	5	The demand signal from the AD-100 passes through a pre-filter which has user set limits for position, rate and acceleration. These limits would prevent overtravel globally (x, y, z, roll, pitch and yaw). After the global signal is converted to actuator commands, each command is again passed through a filter with position, rate and acceleration limits on it. These filters are set up so that if the CS/TMBS command signal cannot equal the demand signal, an alternate trajectory will be generated. The alternate trajectory will maintain the integral relationship between the states and will avoid exceeding the state limits (no overshoot). If the demand returns within the operating envelope, the filters will produce a time optimal trajectory to regain tracking. There are also retract switches on the actuators to cause a hard abort if the actuator travels to a low enough position.

SYSTEM CS/TMBS

SUBSYSTEM INERTIAL MEASUREMENT UNIT

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of Inertial Measurement Unit (IMU)	Startup, operation and shutdown	Loss of gyros or accelerometers mounted on platform	Unable to detect the accelerations and rates of the platform	IV	B	4	The loss of the IMU will not in any way affect the movement of the simulator. It will however cause an immediate shutdown of the simulator. The IMU is tested before liftoff of the simulator, and the CS/TMBS will not start if there is a failure.

SYSTEM CS/TMBS

SUBSYSTEM ANALOG INPUT/OUTPUT

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Loss of analog input signals	Operation	Failure in Analog to Digital converters, loss of input lines	Loss of input terrain signals	IV	C	5	Loss of the analog input signals will present no problems. Unlike the digital signals, when analog signals are lost, the input will drift to zero. The controller will realize the loss of the signal (immediate position error will occur) and will shutdown. It will be extremely rare for analog inputs to be used when a crew is in the simulator (no foreseeable reason).
Loss of analog output signals	Startup, operation and shutdown	Failure of digital to analog converters	Inability to read selected channels of data	IV	C	5	The analog output signals are strictly for the operator to look at data from internally selected variables. They perform no function in the operation of the simulator and their failure poses no problem at all.

SYSTEM CS/TMBS

SUBSYSTEM AD-100 COMPUTER INTERFACE

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of interface between CS/TMBS and the AD-100 computer	Operation	Failure at either the AD-100 or the CS/TMBS transmission end, failure of cable connecting the two	Loss of input signal coming from the AD-100 computer to the CS/TMBS	IV	D	5	Loss of communication between the AD-100 and the CS/TMBS will mean the simulator will all of a sudden lose the command signals. This means the data the CS/TMBS gets will be zero or it could be some very large value. If this occurs during a test, the filters will smooth the data, the limits will prevent overtravel, and the tracking errors will shutdown the simulator. The operator or payload occupants can also shutdown the simulator when this happens. Before the test begins, communication must be first established and therefore no travel will even occur then.
Selection of incorrect data to transmit	Operation	Operator error in selecting the correct data file	The simulator will respond to a different terrain profile than anticipated	IV	D	5	The AD-100 requests the CS/TMBS to send over an identification value for the selected terrain. If the user enters the wrong value, no data will be sent. The only possible error to occur is if the operator selects the wrong data file and enters the corresponding identification value. The only thing that will happen is the simulator will respond to an incorrect set of command signals. No damage will happen from this.

SYSTEM CS/TMBS

SUBSYSTEM ARRAY PROCESSOR

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of array processor	Startup, operation and shutdown	Computer failure of the array processor boards, bus failure in communications between the Supervisor Computer and the array processor	Inability of the Supervisor Computer to perform forward and inverse kinematic transformations, hangup of the multibus	III	D	5	A failure of the array processor will crash the multibus within 10 msec. This will stop the simulator immediately with a soft abort through the Safety Monitor Computer, providing a safe shutdown. The most likely instance of failure would occur during power up, which the Safety Monitor Computer would detect and prevent startup to the simulator. No hazard in itself exists if this happens.
Incorrect data calculations by the array processor	Startup, operation and shutdown	Failure of the program loaded into the ROM of the array processor	The array processor will make incorrect calculations and pass bad values to the Supervisor Computer	III	E	5	The ROM does not change and would not be subject to damage unless there is a major electrical surge through the computer. This is unlikely due to the filtered power supply. Even if bad data was passed from the array processor, the filters and limits on the input signals would prevent dangerous movement of the simulator, and the tracking signals (or the operator or crew) would shutdown the simulator.

SYSTEM CS/TMBS

SUBSYSTEM ENCODER SERVO PROCESSORS

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Failure of Encoder Servo-Processor (ESP)	Startup, operation and shutdown	Computer failure of the ESP	Loss of control of the actuators, loss of the control loops for the actuators	III	D	5	Complete failure of an ESP will cause the CS/TMBS to lose control of that actuator. Each actuator has its own ESP card, so only one actuator would be affected. Loss of the ESP will cause a multi-bus lockup, which would tell the Safety Monitor Computer to shutdown the simulator immediately.
Loss of data stored on the ESP	Startup, operation and shutdown	Failure of the EEPROM on the ESP, bad programming by the operator	The ESP may have the wrong control loop on it to stabilize the actuators, overtravel limits may be corrupted	IV	E	5	The incorrect control loop may cause instability with the simulator. If so, the Inertial Measurement Unit will detect this and shutdown the simulator within 1 second. Poor limits would in itself cause no problem, unless bad data was passed into the simulator. When running while using the AD-100 (the only mode of operations to be used with occupants in the payload) there is an extra set of limits and filters which run on the Supervisor Computer. Thus, there would be no problem here.

SYSTEM CS/TMBS

SUBSYSTEM HYDRAULIC SYSTEM

SUBJECT HAZARD OR UNDESIRED EVENT	PROGRAM PHASE	CAUSE	EFFECT	HAZARD SEVERITY	HAZARD PROBABILITY	RAC	COMMENTS CORRECTIVE ACTION/MINIMIZING PROVISIONS
Loss of servo valve	Startup, operation and shutdown	Clogging of servo, loss of electronic control	Loss of actuator control	IV	C	5	Every actuator has three (3) servo-valves working together to control movement. If one servo was lost, the other two servos would compensate for the loss and no change would be noticed. If more than one servo went out at the same time (highly unlikely), loss of control of the actuator would occur, and the IMU or the Safety Monitor Computer would shutdown the simulator.
Hydraulic pressure variations	Startup, operation and shutdown	Variations in supply voltage to hydraulic pumps, failure in pump, failure in relief valve	Varying output pressure of hydraulic pump, instead of constant 3000 psi	IV	D	5	Short duration pressure pulses are dampened by the accumulators. Sudden sustained low pressure would indicate a large leak. Sustained high pressure would indicate a relief valve malfunction. A pressure compensated pump is designed to de-stroke in the face of increased pressure, eventually going to near zero. The CS/TMBS is equipped with pressure sensors which will shutdown the system in the event of a high or low pressure situation.
Loss of hydraulic pressure	Startup, operation and shutdown	Loss of pump power, blockage in lines, clogged hydraulic filters, burst in hose of failure of release valve	Power to the CS/TMBS will end	III	D	5	Loss of system pressure due to any listed reason implies a decrease in flow volume and hence the actuators would slow down and eventually stop completely as the oil supply from the accumulators is also completed. When the pressure drops below 1500 psi, the Interlock Chassis would detect it, close the system supply valves and servo shutoff valves, open the abort valves, thereby, bringing the simulator to a gentle stop.
Oil leakage	Startup, operation and shutdown	Rupture of hose or manifold, poor seals, etc.	Loss of oil and pressure to simulator	III	D	5	Because of the large reservoir of oil (2500 gallons) any small leak has negligible effect on the CS/TMBS, but would require operator shutdown and repair. A large leak would be noticed by the pump operator or CS/TMBS operator, thus causing a shutdown. If unnoticed, the drop in pressure would cause an automatic shutdown as described above. The crew of the payload is far enough away from any hoses to be safe from rupture.

LIST OF REFERENCES

1) TACOM RDE CENTER Technical Report #13549, "SAFETY ASSESSMENT OF TACOM's CREW STATION/TURRET MOTION BASE SIMULATOR", Alexander A. Reid, April 1991.

2) AR 385-10.

3) MIL-STD-882B.

4) Contraves USA Manual No. IM-27751, "INSTRUCTION MANUAL FOR TACOM", August 1990.

DISTRIBUTION LIST

Copies

Commander 12
Defense Technical Information Center
Bldg. 5, Cameron Station
ATTN: DDAC
Alexandria, VA 22304-9990

Commander 2
U.S. Army Test-Evaluation Command
ATTN: AMSTE-TA-R
Aberdeen Proving Ground, MD 21005-5055

Manager 2
Defense Logistics Studies
Information Exchange
ATTN: AMXMC-D
Fort Lee, VA 23801-6044

Commander
U.S. Army Tank-Automotive Command
ATTN: ASQNC-TAC-DIT (Technical Library) 2
AMSTA-CF (Dr. Oscar) 1
AMSTA-T (Mr. Culling) 1
AMSTA-TBS (Mr. Reininger) 1
AMSTA-RYA (Mr. Janosi) 1
AMSTA-RY (Dr. Beck) 1
AMSTA-RYA (Mr. Reid) 20
Warren, MI 48397-5000

Director
U.S. Material Systems Analysis Activity 1
ATTN: AMXSY-MP (Mr. Cohen)
Aberdeen Proving Ground, MD 21005-5071